«УТВЕРЖДАЮ»
Первый заместитель председателя правления – главный инженер АО «Алмалыкский ГМК»
_____ А. Абдукадыров
«11» 05 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение

СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ.

АО «Алмалыкский ГМК»

на 12 листах

действует с _____

«СОГЛАСОВАНО»

Заместитель председателя правления по безопасности АО «Алмалыкский ГМК»
_____ Р. Саттаров
«11» 05 2022 **г.**

Заместитель председателя правления по цифровизации АО «Алмалыкский ГМК»
_____ А. Азизов
«07» 05 2022 **г.**

Начальник Департамента ИТ АО «Алмалыкский ГМК»
_____ Р. Максумов
«07» 05 2022 г.

И. о. начальника УАП АО «Алмалыкский ГМК»
_____ В. Ирисметов
«06» 05 2022 г.

Главный инженер СТСБ АО «Алмалыкский ГМК»
_____ И. Дятлов
«05» 05 2022 г.

«РАЗРАБОТАНО»

Ведущий инженер по информационной безопасности Отдела безопасности СТСБ АО «Алмалыкский ГМК»
_____ А. Кашутин
«05» 05 2022 г.

г. Алмалык
2022 г.

Оглавление

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Термины, определения и сокращения

ОС	Операционная система
ПО	Программное обеспечение
ТЗ	Техническое задание
ИТ	Информационные технологии
ТП	Техническая поддержка
КИ	Конфиденциальная информация

1.2 Наименование заказчика (пользователя) и поставщика Решения

Заказчик – АО «Алмалыкский ГМК», Республика Узбекистан Ташкентская область инд.110100 г. Алмалык, ул. Амира Темура, 53, e-mail: info@agmk.uz, тел: (998 71) 141-90-09, факс: (998 71) 141-90-33.

Поставщик – Организация (компания), берущая на себя ответственность по поставке и внедрению Решения на условиях первоначального конфигурирования и интеграции с существующими системами, обучение пользователей. Поставщик будет определён по результатам конкурса на отбор наилучшего предложения.

1.3 Основание для приобретения

- Мероприятия по устранению выявленных недостатков информационной безопасности утвержденные Председателем Правления АО «АлмалыкскийГМК» А.Х.Хурсановым от 10.09.2021г. на основании АКТА №13/10712 от 27.07.2021г. по результатам проверки состояния обеспечения информационной и кибербезопасности информационной инфраструктуры АО «Алмалыкский ГМК» от СГБ.

1.4 Плановые сроки начала и окончание работ

Начало – Июль 2022 г.
Окончание – Декабрь 2022 г.

1.5 Порядок оформления и предъявления заказчику результатов работ

Оформление и предъявление Заказчику результатов работ по внедрению Решения осуществляется Поставщиком согласно:

- сетевому графику по реализации проекта;
- требованиям государственных стандартов Республики Узбекистан по оформлению документации;
- требованиям данного Технического задания (ТЗ) с учётом требований, приведённых в подразделах по функциональной части.

Заказчик и Поставщик совместно формируют лист приёмки результатов работ по модулям и функциям системы, на основании которого будет зачитываться успешность реализации проекта. Данный лист приёмки результатов будет включён в договор.

1.6 Источник финансирования

Собственные средства АО «Алмалыкский ГМК».

2. Наименование и цели приобретения решения

Наименование проекта - система предотвращения утечек данных.

Целью является организация оперативного управления и защиты ИТ-активов, а также реагирование на различные рода событий на них, краже конфиденциальной информации, включая внешние и внутренние угрозы. Это повысит защищённость информационных активов Заказчика в целом.

3. Требования к поставщику

Поставщик должен иметь репутацию, достаточный опыт реализации проектов сопоставимого уровня, а также необходимые сертификаты и ресурсы, позволяющие выполнить задание на требуемом уровне, дающем основания полагать, что внедрённое Решение будет принято комиссией.

Поставщик должен соответствовать следующим обязательным требованиям:

- являться авторизованным партнёром производителя Решения в Республике Узбекистан и иметь подтверждающий этот факт сертификат;
- наличие сертифицированного инженера по предоставляемому программному продукту;
- иметь опыт в соответствующих по масштабу проектах;
- иметь соответствующие разрешительные документы (лицензии и сертификаты) для специалистов, принимающих участие в проекте.

Заказчик предоставляет Поставщику необходимые вычислительные ресурсы для инсталляции и внедрения поставляемого Решения в соответствие с рекомендациями, выданными Поставщиком.

4. Требования к решению

Версия поставляемого программного обеспечения должна быть актуальной на дату внедрения его на технических ресурсах Заказчика.

Все комплексы, вновь приобретённые и существующие, должны интегрироваться максимально без остановки систем Заказчика и не должны оказывать перебои в работе существующих систем.

Сдача системы «под-ключ», т.е. с законченным циклом выполнения работ, совместно со специалистами Заказчика, тестирование работоспособности и ввод в коммерческую эксплуатацию.

В предложении должны быть подробно указаны полный перечень выполняемых работ для сдачи проекта «под-ключ».

4.1.1 Требования к Решению в целом

В рамках проекта необходимо предоставление технического решения и его реализация на основе передовых информационных технологий.

По итогу реализации проекта должны быть внедрены следующие системы:

– Система защиты конфиденциальной информации для предотвращения захвата и утечки данных Комбината, и предоставление обеспечения защиты ИТ-активов на 500 пользователей и техническая поддержка от производителя на период не менее 1 года.

Решение должно иметь возможность построения в виртуализированной среде.

Реализация данного решения не должна негативно отразиться на производительности работы приложений Заказчика.

Решение должно учитывать базу передовых тенденций в индустрии информационных технологий.

Должна быть обеспечена возможность дальнейшего расширения охвата

дополнительных систем, серверов и устройств, количества пользователей, наращивания производительности путём добавления вычислительных узлов и/или лицензий.

Система должна иметь возможность консистентного резервного копирования для случаев, когда необходимо сделать возврат к предыдущему состоянию или для случаев сбоя.

4.1.2 Допустимые пределы модернизации и развития Решения

Модернизация Решения должна осуществляться на базе передовых тенденций в индустрии информационных технологий и строиться по принципу открытых систем.

Должна быть обеспечена возможность наращивания общей мощности Решения в соответствии с требованиями, налагаемыми дальнейшим развитием инфраструктуры и введением в эксплуатацию новых приложений.

Интеграция должна происходить без остановки функционирующих систем.

4.1.3 Требования к диагностированию Решения

При вводе в эксплуатацию Решения Поставщик совместно с обслуживающим персоналом Заказчика должен провести полное тестирование и диагностику всех вводимых в эксплуатацию элементов Решения.

В процессе эксплуатации Решения, тестирование и диагностика Решения должны осуществляться персоналом Заказчика.

4.1.4 Требования к перспективе развития и модернизации Решения

Решение должно предусматривать возможность её последующей модернизации при минимальных временных и финансовых затратах по следующим направлениям:

- изменение (дополнение и расширение) форматов и систем;
- расширение списка систем, необходимых к анализу и мониторинга;
- расширение списка автоматизируемых функций;
- адаптация к изменениям норм законодательства и, соответственно, автоматизируемых процессов.

4.2Система предотвращения утечек данных

4.2.1 Назначение системы

Система предотвращения утечек данных (далее DLP) должна послужить как средство для предотвращения захвата и утечки данных комбината, и предоставление обеспечения защиты от различных кибератак.

4.2.2 Общие требования

Программное обеспечение для защиты информации (DLP – система) должна обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. Система должна анализировать все данные, передаваемые работниками как внутри, так и за пределы информационной сети Заказчика.

Програмное обеспечение должно обеспечивать возможность поиска конфиденциальной информации, находящейся на рабочих станциях и файловых серверах.

ПО должно контролировать следующие каналы потенциальной утечки конфиденциальной информации:

• исходящие SMTP-соединения (блокировка агентским модулем исходящих почтовых сообщений по протоколу SMTP(S));

• исходящие HTTP-соединения;

• исходящие HTTP-соединение (сообщения в форумах и социальных сетях, посещенные сайты, отправленные файлы); web-коммункации (gmail.com, rambler.ru, yahoo.ru, yandex.ru, mail.ru);

•возможность установки режима перехвата: только шифрованный либо нешифрованный трафик, весь трафик;

•возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (с использованием контентного и атрибутивного анализа);

•копирования информации на внешние носители информации и информационные ресурсы (с возможностю блокирования записи файлов на съёмные носители по содержимому передаваемой информации);

•печать информации на локальном/сетевом/виртуальном принтере (возможность блокировки документов по содержимому документа).

• мессенджеры: Skype, Telegram (перехват текстовых сообщений, файлов (включая веб-версию), перехват голосовых сообщений) WhatsApp, Google Hangouts, SIP, Viber, MS Lync, OSCAR, XMPP, MRA, YIM; Slack; Discord; Zoom.

ПО должно обеспечивать следующие функциональные возможности:

- предотвращения разглашения конфиденциальной информации через корпоративную почтовую систему;
- возможность блокировки исходящих писем, содержащих конфиденциальную информацию;
- предотвращения разглашения конфиденциальной информации через корпоративную систему доступа в сеть Интернет;
- возможность извлечения конфиденциальной информации с HTTP-/ HTTPS-трафика;
- возможность блокировки HTTP-/ HTTPS-трафика;
- предотвращения разглашения конфиденциальной информации и мониторинг каналов утечки, а именно: копирование конфиденциальной информации с сетевой папки на локальне жесткие диски, копирование конфиденциальной информации на съемные носители, отправка конфиденциальной информации на локальную и сетевую печать, а также по факсу, защита содержимого буфера обмена при операциях копирования/ вставки;
- возможность сканирования (в том числе - по заданному расписанию) локальных жестких дисков конечного узла сети на предмет наличия конфиденциальной информации;
- возможность распознавания текстовой информации находящейся в графических объектах (pdf-файлы, изображения и т.д.), а также графических образов в таких объектах (подписей ответственных лиц, штампов, логотипов и т.п.);
- возможность извлечения текстового содержимого из аудиофайлов разговоров перехваченных в мессенджерах Skype, MS Lync, Viber, Zoom, MS Teams, Telegram, WhatsApp а также в программах IP-телефонии использующих протокол SIP
- возможность создания цифровых отпечатков документов для последующего обнаружения в перехваченных данных похожих документов

- возможность самообучения на документах, с последующим блокированием похожих документов;
- возможность автономной работы клиентов и модулей ПО (серверов детектирования), в случае отключения конечного узла от корпоративной сети или потери соединения с сетью;
- возможность централизованного администрирования политик безопасности;
- возможность оперативного внесения изменений в режиме реального времени в политики безопасности ПО, изменения существующих и добавление новых правил, настроек;
- настройка автоматических сообщений о нарушениях политик ПО (с уведомлением в Telegram);
- настройки различных вариантов реагирования на нарушени политики безопасности;
- настройка и генерация отчетов по датам, фактам нарушения политик безопасности;
- возможность работать с консолью управления на русском языке;
- возможность использовать учетные записи существующей Active Directory для аутентификации в консоли управления;
- возможность просмотра атрибутов учетных записей AD (имя, телефон, департамент, должность и т.д.) непосредственно из консоли.

4.2.3 Технические требования

Возможности контроля операций:

- Запись конфиденциальной информации (далее - КИ) на съемные носители (USB, CompactFlash, SD);
- контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.);
- Печать КИ (сетевые и локальне, виртуальные принтеры);
- Копирование КИ в буфер обмена (возможность блокирования как копирования, так и вставки файлов по содержимому);
- Запись КИ на локальные диски;
- Запись КИ на CD/DVD;
- Контроль обращения приложений к КИ (в том числе передача файлов, содержащих КИ через Skype, Teams, Zoom, Telegram, Watsapp и т.д.)
- Отправка КИ данных через HTTP протокол;
- Отправка КИ данных через HTTPS протокол;
- Контроль SMTP на уровне почтовых клиентов;
- Копирование КИ файлов на сетевые ресурсы, в том числе облачные ресурсы и контроль файлового хранилища MS Onedrive;
- Контроль функции PrintScreen, снятия скриншотов при нажатии клавиши PrintScreen

Возможность настройки и применения политик и конфигураций агенту на конечных точках по местунахождения: в корпоративной сети, или за пределами корпоративной сети.

Возможность контроля массового копирования документов на внешние носители. Система должна контролировать количество файлов, которые пользователь может копировать на внешний носитель в течение установленного периода времени.

Возможность шифрования трафика между консолями

Возможность аутентификации пользователей, работающих с системой, на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему).

Возможность блокировки подключения устройств с определенными параметрами.

Под контролем подразумевается возможность как детектирования КИ, так и блокировки (препятствование передачи) КИ (в соответствии с заданными политиками).

Возможность развертывания (установки) модулей агентов детектирования на ОС Windows и Linux.

Возможность реакции на инциденты: автоматическое сообщение ответственного лица или владельца информации, блокирование отправки по электронной почте, блокировка отправки данных через веб-формы, выполнение скрипта, удаления конфиденциальной информации.

Возможность запуска дополнительных действий при возникновении инцидентов (скриптов).

Возможность хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL, MySQL, SQLite.

Возможность настройки правил записи данных в базы для регуляции, в какую базу или группу баз записывать информацию в зависимости от типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой информации.

Распознавание речи (анализ текстового содержимого перехваченных аудиоразговоров)

Распознавание (OCR – Optical Character Recognition) должно обеспечиваться встроенной технологией/механизмом без использования дополнительного програмного обеспечения сторонних производителей.

Распознавание текста должно поддерживать алфавит на латинице и кириллице с поддержкой английского, русского и узбекского языков.

Распознавания и преобразования отсканированных образов в следующих форматах: PDF, BMP, JPEG, PNG, TIFF.

Направления работы OCR:

- Локальное сканирование;
- Копирование КИ на внешние носители;
- Копирование КИ на Файловый сервер;
- Отправка КИ через HTTP/HTTPS;
- Отправка КИ через Webmail протокол;
- Отправка через SMTP протокол;

Возможность регулировать уровень доступа пользователей к USB с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.);

Возможность развертывания модуля конечних точек на системах Ubuntu с возможностью: перехват сетевого трафика (SSL/TLS, SMTP, POP3, FTP, HTTP, XMPP, IMAP), захват нажатий клавиатуры, захват снимков экрана (с точностью до секунды), контроль и аудит usb-устройств.

- Выявление КИ, которая находится в состоянии покоя;
- Контроль утечки КИ на сменные носители в том числе блокировку и логирования такой информации;
- Контроль утечки КИ через HTTP/HTTPS каналы;
- Контроль утечки КИ через Webmail протокол.

Программное обеспечение должно поддерживать возможность превентивного информирования администратора, когда пользователь вставляет ненадежный USB накопитель в компьютер.

Агент програмного обеспечения должен поддерживать работу в безопасном режиме, все процессы должны быть скрыты от конечного пользователя, а также файлов и папок агента на компьютере пользователя

4.2.4 Требования к интерфейсу

Программное Обеспечение должно поддерживать следующие языкии интерфейса: английский, русский.

Программное Обеспечение должно поддерживать централизованное управление компонентами системы из консолей: единая консоль администратора и единая консоль офицера безопасности.

4.2.5 Требования к классификации

Система должна относить приложения, используемые контролируемыми пользователями к категориям.

Система должна относить сайты, посещенные пользователями к категориям.

Программное обеспечение должно классифицировать не только файлы, а также папки в режиме реального времени.

Программное обеспечение должно контролировать копирование файлов на уровне буфера обмена и иметь возможность блокировать такую операцию в зависимости от уровня классификации файла.

Программное беспечение должно контролировать снимок экрана файлов Microsoft Office

4.2.6 Дополнительные требования

Программное обеспечение должно поддерживать:

- Перехват почты, отправляемой через почтовые сервера, развернутые на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного

обеспечения, путем интеграции с почтовыми серверами по протоколам POP3, IMAP, SMTP, а также при помощи коннектора MS Exchange

- интеграцию с посторонними веб-сервисами (шлюзами) с помощью специализированных стандартних протоколов (ICAP).
- контроль облачных хранилищ (iCloud, Dropbox, GoogleDrive, OneDrive, Диск-О (в т.ч. ОблакоMail.ru), Яндекс.Диск)
- Система должна позволять выполнять аудит операций с файлами и папками. Операции с файлами: создание, чтение, запись, удаление, переименование, открытие, изменение прав доступа. Операции с папками: создание, удаление, переименование, открытие, изменение прав доступа
- В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных, система должна иметь возможность гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы.
- Обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах.
- Автоматический запуска программ и скриптов при срабатывании правил безопасности.

Исполнитель должен иметь возможность обеспечить в рамках технической поддержки (ТП) внедрение и настройку системы у Заказчика в полном объеме с предоставлением консультационной поддержки по эксплуатации и администрирования системы и ее составляющих.

Требования к ТП системы:

- ТП должна обеспечиваться в режиме 24x7 ;
- ТП должна предоставляться на русском языке;

Внедрение и настройка системы у Заказчика в полном объеме с предоставлением консультационной поддержки не менее чем трем специалистам Заказчика по эксплуатации и администрирования системы и ее составляющих;

Проведение технических консультаций персонала Заказчика (не менее 3х человек) по установке и настройке (системы) предотвращения утечки конфиденциальной информации;

Агент поддерживает работу в автономном режиме, в случае отсутствия соединения между компонентами системы или с внешними сетями, при этом перехваченные данные хранятся в локальном хранилище с возможностями ограничения размера локального хранилища и срока хранения данных в нем

Индивидуальные настройки работы агентов для отдельных учетных записей пользователей, компьютеров и групп Active Directory

Активация настроек агента по условиям: недоступность сервера в течении некоторого времени, активное vpn-подключение, пользовательское условие, задаваемое при помощи Lua-скрипта.

Должна бать реализована функция перехвата трафика с помощью агента, а не с помощью установки плагина на браузер пользователя.

5. Порядок контроля и приёмки системы

5.1 Требования к реализации поставляемого решения

Поставщик Решения должен согласовать план реализации с Заказчиком.

Поставщик Решения должен предоставить Заказчику технические требования по интеграции поставляемого Решения с инфраструктурным оборудованием Заказчика.

Заказчик должен провести полную проверку работоспособности набора функциональности Решения прежде, чем начать процедуру приёмки предоставленного решения.

Поставщик должен произвести необходимые тесты по производительности поставленного Решения для проверки соответствия заявленным характеристикам и функциональности указанных в данном документе.

Решение о приёмке продукта принимается только после того, как Поставщик произвёл первоначальную настройку системы и продемонстрировал корректную работу всей функциональности.

5.2 Порядок сдачи и приёмки результатов работ и услуг

Оказанные услуги Поставщик оформляет актом выполненных работ (услуг) согласно проекту, согласовывает с Заказчиком и предоставляет Заказчику счёт-фактуру на сумму выполненных работ (услуг) и двухсторонне оформленные акты выполненных работ (услуг) по проекту.

6. Требования по передаче технических и иных документов по завершению и сдаче результатов работ и услуг

По завершению работ Поставщик передаёт Заказчику следующие документы:

- инструкции для администраторов систмы;
- инструкции по установке и настройки системы;
- инструкции по активации лицензий;
- лицензионный сертификат;
- лицензионный ключ.

7. Требования по техническому обучению поставщиком персонала заказчика по результатам выполненных работ и оказанных услуг

Поставщик обеспечивает подготовку обслуживающего персонала Заказчика в количестве 2 человек к работе по сопровождению Решения путём проведения:

- семинаров по теоретическим основам работы (настройки, сопровождение приобретаемого программного обеспечения);
- обучающихсеминаров;
- практики на рабочем месте.

Все вышеуказанные варианты подготовки персонала Заказчика могут проводится с использованием онлайн технологий системы дистанционного обучения (СДО).

8. Авторские права с указанием условий о передаче неисключительных прав на объекты интеллектуальной собственности, возникших в связи с исполнением обязательств поставщика по выполнению работ и оказанию услуг

После ввода Решения в эксплуатацию, Поставщик передаёт неисключительное право на пользование Решения на срок согласно договору (электронные ключи). Приёмка лицензионных прав осуществляется актом приёма передачи соответствующих лицензий в объёме, указанном согласно заключённого договора между Заказчиком и Поставщиком.

Неисключительные права на использование Решения должны передаваться с возможностью скачивания дистрибутивов ПО с официального сайта компании производителя Решения.

Требования к патентной и лицензионной чистоте: ПО должно состоять из экземпляров, которые распространяются и используются в объёмах и на условиях, определённых в лицензиях.

9. Требования по стандартизации и унификации

При эксплуатации Решения должны использоваться технические средства, операционные системы, системы управления базами данных, позволяющие построить единое информационное пространство в рамках Заказчика и обеспечивающих прозрачность доступа к данным.

Стандартизация и унификация технических средств системы должны обеспечиваться посредством использования серийно выпускаемых средств вычислительной техники и коммуникационного оборудования.